ACCESS CONTROL FOR HARDWARE UNITS

BACKGROUND

[0001] Delivery of applications to computers and mobile devices like smart phones has become easier with the birth of application stores. From these on-line stores, it is possible to purchase and download an application to the device in a simple manner without the requirement complex installation or configuration procedures. At the same time, the capabilities of different devices have increased, and the devices now commonly offer features like a high-resolution camera, fast access to internet services, ability to access e-mail and process documents and so on. New applications make use of these resources of the device.

[0002] For various reasons, it may be desirable to limit the application's access to the resources of the device. For example, it may be desirable to disable the application's access to the camera or microphone of the device for privacy reasons. Furthermore, access to communication functionalities may be prevented to avoid excessive communication costs. Generally, data security of devices, e.g. against malicious software like viruses and spyware is a concern.

[0003] There is, therefore, a need for solutions for providing access control to the resources of user devices.

SUMMARY OF THE INVENTION

[0004] Now there has been invented an improved method and technical equipment implementing the method, by which the above problems are alleviated. Various aspects of the invention include a method, an apparatus and a computer readable medium comprising a computer program stored therein, which are characterized by what is stated in the independent claims. Various embodiments of the invention are disclosed in the dependent claims.

[0005] The invention relates to providing access control to service units of a computer system. When a program unit such as a process or a thread accesses a service unit, the service unit generates an access signal (e.g. an interrupt) indicating the service unit has been accessed. This access signal is handled e.g. by an interrupt handling arrangement at the processor, and in case the program unit is not authorized to access the service unit, the program unit is terminated.

[0006] The service unit may be a hardware unit such as a processing unit, a processor block, a communications unit, a data storage unit, a camera, and a microphone. The hardware unit may have a line for generating an interrupt to the processor, that is, a line that is configured to be connectable to an interrupt line of the processor. The interrupt line may be a hardware interrupt line or a software interrupt line. The processor may mask the interrupts when the program unit is authorized to access the hardware unit, and otherwise the interrupt may be processed by an interrupt handler. The interrupt handler may be configured to terminate the accessing process (the program unit) so that when an unmasked interrupt is received, it is deemed that the process has no access rights. In other words, an interrupt signal may be used to indicate access from a process to a hardware unit, and the process may be terminated if the access was unauthorized.

[0007] According to a first aspect there is provided a method comprising accessing from a program unit a service unit for service, receiving an access signal related to the service unit in response to the accessing, determining whether the accessing is authorized, and if the accessing is not authorized, terminating the program unit.

[0008] According to an embodiment, the service unit is a hardware unit and the access signal is a hardware signal such as a hardware interrupt from the service unit. According to an embodiment, the signal is a software interrupt or a software exception from the service unit. According to an embodiment, the signal comprises information indicative of the program unit. According to an embodiment, the signal is an interrupt and the method comprises setting up an interrupt handler for handling the interrupt, receiving the interrupt, handling the interrupt in the interrupt handler, and terminating the program unit with the interrupt handler. According to an embodiment, the method comprises setting up the interrupt handler in response to the program unit not having rights to access the service unit, and masking the interrupt in response to the program unit having rights to access the service unit. According to an embodiment, the accessing is authorized if the program unit has rights to access the service unit. According to an embodiment, the accessing comprises transferring data with the service unit such as receiving data, storing data or processing data, or the accessing comprises sending one or more control signals to a service unit. According to an embodiment, the program unit comprises at least one from the group of a thread, a process, an application and a user shell. According to an embodiment, the service unit comprises at least one from the group of a processing unit, a processor block, an i/o unit, a data storage unit, a camera, and a microphone. According to an embodiment, the terminating comprises alerting a user of the accessing or of the terminating. According to an embodiment, the method comprises executing the program unit in a pre-emptive environment, wherein the program unit is set for execution in at least a first time period and at a second time period, and during the first and second time period another program unit being set for execution in the pre-emptive environment, accessing from a program unit a service unit for service during the first time period, receiving the access signal during the first time period, and terminating the program unit during the first time period.

[0009] According to a second aspect there is provided an apparatus comprising at least one processor, at least one memory including computer program code for one or more program units, the at least one memory and the computer program code configured to, with the processor, cause the apparatus to at least access from a program unit a service unit for service, receive an access signal related to the service unit in response to the accessing, determine whether the accessing is authorized, and if the access is not authorized, terminate the program unit.

[0010] According to an embodiment, the apparatus comprises a hardware signal line for receiving the access signal from the service unit, wherein the service unit is a hardware unit and the access signal is a hardware signal such as a hardware interrupt. According to an embodiment, the signal is a software interrupt or a software exception from the service unit, and the apparatus further comprising computer program code configured to, with the at least one processor, cause the apparatus to receive a software interrupt in response to the access. According to an embodiment, the signal comprises information indicative of the program unit. According to an embodiment, the signal is an interrupt and the apparatus further comprises computer program code configured to, with the at least one processor, cause the apparatus to set up an interrupt handler for handling the interrupt, receive the inter-